PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-274232
(43)Date of publication of application : 30.09.2004

(51)Int.Cl. H04L 12/28

(21)Application number : 2003-060022
(22)Date of filing : 06.03.2003

(71)Applicant : CANON INC
(72)Inventor : YAMAMOTO TETSUYA

(54) RADIO COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To apply an information input/output apparatus to a secure radio LAN system without greatly increasing the component cost/software developing man-hour.
SOLUTION: The radio communication system is composed of an authenticator for authenticating with a password and one or more terminals, each composed of one or more first radio communication units, and one or more second radio communication units wired to the authenticator. Each radio communication unit has a function for operating in at least two communication modes. There is no interconnection between the communication modes, i.e., the radio communication unit operating in the first communication mode and the radio communication unit operating in the second communication mode cannot communicate with each other. Using such radio communication units, a series of communications for sending information such as passwords to be used for the authentication are made in the first communication mode, and other communications are made in the second communication mode.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-274232
(P2004-274232A)
(43)公開日　平成16年9月30日(2004.9.30)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/28	H04L 12/28	300Z	5K033
	H04L 12/28	303	
	H04L 12/28	307	

審査請求 未請求　請求項の数 10　OL　（全 10 頁）

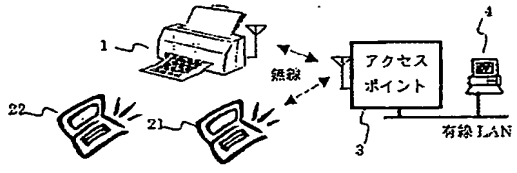
(21)出願番号　特願2003-60022 (P2003-60022)
(22)出願日　平成15年3月6日 (2003.3.6)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　山本　哲也
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

Fターム(参考)　5K033 AA08 CC01 DA01 DA17 DB12 DB14 DB16 DB18 DB19

(54)【発明の名称】無線通信システム

(57)【要約】
【課題】パスワード認証を用いて安全な通信を行う参加ＬＡＮシステムにおいて、キーボード等の文字入力手段をもたない装置もこの無線ＬＡＮシステムに参加させる。
【解決手段】文字入力手段をもたない装置のユーザ名・パスワード登録をアドホックモードで行う。それ以外のデータ送受信はインフラストラクチャモードで行う。それ以外のデータ送受信はインフラストラクチャモードで行う。
【選択図】　図１



【特許請求の範囲】

【請求項１】

パスワード認証を行う認証装置と、前記認証装置に有線接続された１台以上の第一の無線通信装置と、第二の無線通信装置を備えた１台以上の端末装置からなる無線通信システムにおいて、各無線通信装置は少なくとも２つの通信モードで通信する機能を備えており、認証に用いられる情報の送受は第一の通信モードで行われ、それ以外の通信は第二の通信モードで行われることを特徴とする無線通信システム。

【請求項２】

パスワード認証を行う認証装置と、前記認証装置に有線接続された１台以上の第一の無線通信装置と、１台以上の第二の無線通信装置と、前記第二の無線通信装置に有線接続された１台以上の端末装置からなる無線通信システムにおいて、各無線通信装置は少なくとも２つの通信モードで通信する機能を備えており、認証に用いられる情報の送受は第一の通信モードで行われ、それ以外の通信は第二の通信モードで行われることを特徴とする無線通信システム。

【請求項３】

前記認証装置と前記端末装置とが通信モード切替手段を備えることを特徴とする、請求項１または２に記載の無線通信システム。

【請求項４】

前記第一の通信モードにおいて、前記認証装置から前記端末装置にユーザ名とパスワードを含む情報を送る工程が含まれることを特徴とする、請求項１、２または３に記載の無線通信システム。

【請求項５】

前記第一の通信モードにおいて、前記端末装置から前記認証装置にユーザ名を含む情報を送る工程と、前記認証装置から前記端末装置にパスワードを含む情報を送る工程が含まれることを特徴とする、請求項１、２または３に記載の無線通信システム。

【請求項６】

前記第一の通信モードにおいて、前記端末装置から前記認証装置にユーザ登録要求を含む情報を送る工程が含まれることを特徴とする、請求項４または５に記載の無線通信システム。

【請求項７】

前記第一の通信モードにおいて、前記第一の通信装置から前記端末装置にユーザ名とパスワードを含む情報を送る工程が含まれることを特徴とする、請求項１、２または３に記載の無線通信システム。

【請求項８】

前記第一の通信モードにおいて、前記端末装置から前記第一の通信装置にユーザ名を含む情報を送る工程と、前記第一の通信装置から前記端末装置にパスワードを含む情報を送る工程が含まれることを特徴とする、請求項１、２または３に記載の無線通信システム。

【請求項９】

前記第一の通信モードにおいて、前記端末装置から前記第一の通信装置にユーザ登録要求を含む情報を送る工程が含まれることを特徴とする請求項７または８に記載の無線通信システム。

【請求項１０】

前記第一の通信モードがＩＥＥＥ８０２．１１のアドホックモードであり、前記第二の通信モードがＩＥＥＥ８０２．１１のインフラストラクチャモードであることを特徴とする、請求項１乃至請求項９のいずれかに記載の無線通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は無線通信システムに関する。特に、無線ＬＡＮシステムに好適である。

【０００２】

【従来の技術】

複数台のコンピュータからなるシステムにおいて、情報共有やプリンタ等情報処理機器の有効活用の為にＬＡＮを構築することが一般的になりつつある。近年，ＬＡＮの一部もしくは全部を無線化した無線ＬＡＮシステムが次第に利用されるようになってきている。ＬＡＮケーブルの敷設が不要である事、ノート型ＰＣなどの可搬型情報処理機器の利便性を鑑みると、無線ＬＡＮは今後さらに利用が拡大するものと考えられる。

【０００３】

無線ＬＡＮにおいては、情報信号が空気中を伝わるため、有線ＬＡＮと比較して不正アクセスを受ける危険が高まる。

【０００４】

この対策として、ＥＡＰ（Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）と、ＩＥＥＥ８０２．１Ｘ［２００１年９月時点の名称］とを用いる無線ＬＡＮシステムがある。このシステムには認証サーバが存在し、このサーバがユーザ管理と暗号鍵管理を行っている。これにより、ユーザ名とパスワードによってシステムに認証されたユーザだけが無線ＬＡＮ端末を介してネットワークに接続することができ、かつ認証されたユーザが送受信するデータは悪意の第三者が見ることができないように暗号化された、安全な無線ＬＡＮシステムが構築できる。

【０００５】

【発明が解決しようとする課題】

上記の安全な無線ＬＡＮシステムは、ユーザ名とパスワードとをユーザが入力することを想定している。このためには無線ＬＡＮ端末はキーボードのような文字入力手段を備えている必要がある。

【０００６】

端末装置の一種である、スキャナやプリンタといった情報入出力装置は、一般にはキーボードのような文字入力手段を備えていない。

【０００７】

情報入出力装置をそのまま上記の安全な無線ＬＡＮシステムに適用するには、これらの装置に文字入力手段を追加する必要があり、部品コストが増加する。パスワード認証以外の認証方式を用いれば文字入力手段は必要なくなるかもしれないが、別の認証方式を実現するためのソフトウェアが必要となり、開発工数が増加する。

【０００８】

本発明は上述の課題に鑑みてなされたもので、その目的とするところは、部品コスト・ソフトウェア開発工数の大幅な増加を伴わずに、情報入力出力装置を上記の安全な無線ＬＡＮシステムに適用することである。

【０００９】

【課題を解決するための手段】

上記目的を達成するため、本出願にかかる第一の発明の無線通信システムは、パスワードによる認証を行う認証装置と、前記認証装置に有線接続された１台以上の第一の無線通信装置と、第二の無線通信装置を備えた１台以上の端末装置からなる。各無線通信装置は少なくとも２つの通信モードで通信する機能を備えている。ここで、各通信モード間では相互接続性がない。即ち、第一の通信モードで動作している無線通信装置と、第二の通信モードで動作している無線通信装置とは通信を行うことができない。このような無線通信装置を用いて、パスワード等の，認証に用いられる情報を伝える一連の通信は第一の通信モードで行われ、それ以外の通信は第二の通信モードで行われることを特徴とする。

【００１０】

従来例では、認証サーバで発行されたパスワード等の情報は、ユーザが覚えておくものであり、無線でやり取りされることはない。前記端末装置であるところの情報入出力装置に関して、それらの情報が第一の通信モードで送受信される。第一の通信モードで送受信される情報には、パスワード発行要求，ユーザ名，ＩＥＥＥ８０２．１１におけるＥＳＳＩＤのような無線通信識別情報等が含まれる場合もある。従来例において無線でやり取りさ

れていた情報が、第二の通信モードで送受信される。

【００１１】

本出願にかかる第二の発明は、パスワードによる認証を行う認証装置と、前記認証装置に有線接続された１台以上の第一の無線通信装置と、１台以上の第二の無線通信装置と、前記第二の無線通信装置に有線接続された１台以上の端末装置からなる。各無線通信装置は少なくとも２つの通信モードで通信する機能を備えている。ここで、各通信モード間では相互接続性がない。第一，第二の無線通信装置を用いて、パスワード等の，認証に用いられる情報を伝える一連の通信は第一の通信モードで行われ、それ以外の通信は第二の通信モードで行われることを特徴とする。

【００１２】

本出願にかかる第三の発明は、第一乃至第二の発明に係り、前記認証装置と前記端末装置とが通信モード切替手段を備えることを特徴とする。これにより、操作者の操作またはプログラムに基づいて通信モードを変更することが可能となる。

【００１３】

本出願にかかる第四の発明は、第一乃至第三の発明に係り、前記第一の通信モードにおいて、前記認証装置から前記端末装置にユーザ名とパスワードを含む情報を送る工程が含まれることを特徴とする。

【００１４】

本出願にかかる第五の発明は、第一乃至第三の発明に係り、前記第一の通信モードにおいて、前記端末装置から前記認証装置にユーザ名を含む情報を送る工程と、前記認証装置から前記端末装置にパスワードを含む情報を送る工程が含まれることを特徴とする。

【００１５】

本出願にかかる第六の発明は、第四乃至第五の発明に係り、前記第一の通信モードにおいて、前記端末装置から前記認証装置にユーザ登録要求を含む情報を送る工程が含まれることを特徴とする。

【００１６】

本出願にかかる第七の発明は、第一乃至第三の発明に係り、前記第一の通信モードにおいて、前記第一の通信装置から前記端末装置にユーザ名とパスワードを含む情報を送る工程が含まれることを特徴とする。

【００１７】

本出願にかかる第八の発明は、第一乃至第三の発明に係り、前記第一の通信モードにおいて、前記端末装置から前記第一の通信装置にユーザ名を含む情報を送る工程と、前記第一の通信装置から前記端末装置にパスワードを含む情報を送る工程が含まれることを特徴とする。

【００１８】

本出願にかかる第九の発明は、第七乃至第八の発明に係り、前記第一の通信モードにおいて、前記端末装置から前記第一の通信装置にユーザ登録要求を含む情報を送る工程が含まれることを特徴とする。

【００１９】

【発明の実施の形態】

以下に、図面を参照して、この発明の好適な実施の形態を例示的に詳しく説明する。ただし、この実施の形態に記載されている構成要素はあくまで例示であり、この発明の範囲をそれらのみに限定する趣旨のものではない。

【００２０】

（第一の実施の形態）

本発明の第一実施の形態は図１の構成をとる無線ＬＡＮシステムである。本無線ＬＡＮシステムは、ＩＥＥＥ８０２．１１ｂに準拠しており、より高い情報セキュリティのためにＥＡＰとＩＥＥＥ８０２．１Ｘを用いている。１は無線ＬＡＮ通信機能を備えたプリンタ、２１～２２は無線ＬＡＮ通信機能を備えたコンピュータ、３はプリンタ１やコンピュータ２１～２２といった無線ＬＡＮ端末間の通信を中継したり、無線ＬＡＮと有線ＬＡＮと

の中継を行ったりする為のアクセスポイント、４は認証サーバである。
【００２１】
無線ＬＡＮ通信部は、ＩＥＥＥ８０２．１１ｂに準拠しているので、インフラストラクチャモードとアドホックモードのどちらのモードでも通信できる。インフラストラクチャモードとは、アクセスポイントが親局の役割を持ち、無線ＬＡＮ端末の通信には必ずアクセスポイントを介して通信するモードである。アドホックモードとは、アクセスポイントも含めてすべての無線ＬＡＮ通信部が対等な立場になって、１対１で通信するモードである。
【００２２】
プリンタ１，コンピュータ２１，２２をネットワークに接続するには、認証サーバ４が管理しているユーザ名とパスワードによって認証される必要がある。
【００２３】
コンピュータ２１，２２に関しては、新規ユーザを登録する場合、システム管理者は新規ユーザ名とパスワードを認証サーバ４に登録する。新規登録されたユーザはコンピュータ２１，２２のキーボードに自ユーザ名とパスワードを入力する。ユーザ名とパスワードが正しければ認証が成功し、このユーザはネットワークに接続できる。
【００２４】
プリンタ１に関しては、このプリンタに固有のユーザ名とパスワードを割り当てる。このために以下の工程を踏む（図２）。
【００２５】
（１）システム管理者はプリンタ１を操作して、これの通信モードをアドホックモードに設定し、アクセスポイント３または認証サーバ４を操作して、アクセスポイント３の通信モードをアドホックモードに設定し、通信チャネルを両者同じチャネルに設定する（Ｓ１０１）。
【００２６】
（２）システム管理者は認証サーバ４を操作して、プリンタ１に対応する固有のユーザ名とパスワードを生成し、これらを所定のアクセスポイント３を介して送信する。ＩＥＥＥ８０２．１１ｂにおけるＥＳＳＩＤも送信する（Ｓ１０２）。
【００２７】
（３）プリンタ１は上記データを受信する（Ｓ１０３）と、これらを自身の記憶手段に保持し、これらを受信した旨を出力する（Ｓ１０４）。出力は、プリンタ１のＬＥＤ等の出力手段に出力してもよいし、受信した旨の情報を送信してアクセスポイント３または認証サーバ４の出力手段に出力するものであってもよい。
【００２８】
（４）所定の時間がたっても上記の出力がない場合（Ｓ１０５）は、再度プリンタ１に対応する固有のユーザ名とパスワードを生成し、これらを送信する。これらは前回送信したものと同じであってもよいし、異なるものであってもよい。ＥＳＳＩＤも再度送信する（Ｓ１０２）。
【００２９】
（５）上記の出力を確認の後、プリンタ１の通信モードをインフラストラクチャモードに設定し、アクセスポイント３の通信モードをインフラストラクチャモードに設定する。これらの設定は、システム管理者の操作によるものでもよいし、プログラムによって自動で行われてもよい（Ｓ１０６）。
【００３０】
（６）プリンタ１は上記ユーザ名とパスワードを用いてネットワークに接続する（Ｓ１０７）。
【００３１】
アドホックモードでの通信データは、暗号化データでも平文データでも構わない。
【００３２】
プリンタ１を正式にネットワークから切断するときは、システム管理者が認証サーバを操

作して、プリンタ１を示すユーザをログアウトさせる。

【００３３】

システムに２台以上の上記のプリンタがある場合でも、各プリンタに対して上記の手続きにより、ネットワークに接続できる。各プリンタのＩＤは認証サーバが一元管理しているので、ネットワーク内のどのアクセスポイントを経由しても上記の手続きが可能となる。

【００３４】

ユーザ名・パスワードの発行には認証サーバ４にアクセスできる必要がある為，システム管理者だけがユーザ名とパスワードを発行できる。これらのデータが送受されるアドホックモードの期間は短く、さらにアドホックモードの開始時点はシステム管理者にゆだねられているので、第三者がユーザ名とパスワードを傍受することは困難である。通信チャネルを第三者が知ることも困難である。これにより安全な無線ＬＡＮシステムが維持できる。

【００３５】

(第二の実施の形態)

本発明の第二実施の形態は図３の構成をとる無線ＬＡＮシステムである。本無線ＬＡＮシステムは、ＩＥＥＥ８０２．１１ｂに準拠しており、より高い情報セキュリティのためにＥＡＰとＩＥＥＥ８０２．１Ｘを用いている。１０１はプリンタ、１０２はプリンタに接続された無線ＬＡＮユニット、２１～２２は無線ＬＡＮ通信機能を備えたコンピュータ、３は無線ＬＡＮユニット１０２やコンピュータ２１～２２といった無線ＬＡＮ端末間の通信を中継したり、無線ＬＡＮと有線ＬＡＮとの中継を行ったりする為のアクセスポイント、４は認証サーバである。

【００３６】

無線ＬＡＮ通信部は、ＩＥＥＥ８０２．１１ｂに準拠しているので、インフラストラクチャモードとアドホックモードのどちらのモードでも通信できる。

【００３７】

プリンタ１，コンピュータ２１，２２をネットワークに接続するには、認証サーバ４が管理しているユーザ名とパスワードによって認証される必要がある。

【００３８】

コンピュータ２１，２２に関しては、新規ユーザを登録する場合、システム管理者は新規ユーザ名とパスワードを認証サーバ４に登録する。新規登録されたユーザはコンピュータ２１，２２のキーボードに自ユーザ名とパスワードを入力する。ユーザ名とパスワードが正しければ認証が成功し、このユーザはネットワークに接続できる。

【００３９】

プリンタ部に関しては、このプリンタ部に固有のユーザ名とパスワードを割り当てる。このために以下の工程を踏む（図４）。

【００４０】

（１）プリンタ１０１のシステムリセットを掛けることにより、再起動時にはプリンタ１０１に接続された無線ＬＡＮユニット１０２がアドホックモードで動き始める。システム管理者はアクセスポイント３または認証サーバ４を操作して、アクセスポイント３の通信モードをアドホックモードに設定し、通信チャネルを両者同じチャネルに設定する（Ｓ２０１）。

【００４１】

（２）プリンタ１０１からは、自身をネットワークに参加させるために、ユーザ登録要求データが送信される（Ｓ２０２）。認証サーバ４はユーザ登録要求データを受け取る（Ｓ２０３）と、受け取った旨の応答データを送信する（Ｓ２０４）。プリンタ１０１は所定の時間内に認証サーバ４からの応答がない場合（Ｓ２０５）は、応答受信失敗回数が所定値より少ないことを確認（Ｓ２０６）した後、Ｓ２０２に移る。プリンタ１０１からのデータ送信を所定の回数行っても応答がない場合（Ｓ２０６）、あるいは最初のデータ送信から所定の時間が経過しても認証サーバ４からの応答がない場合、プリンタ１０１はこのフェーズの通信が失敗した旨のメッセージを出力する（Ｓ２０７）。

（３）認証サーバ４からの応答を受信した場合（Ｓ２０５）は、プリンタ１０１は自身を表すユーザ名を送信する（Ｓ２０８）。このユーザ名には、プリンタ自身が持つＩＤ、プリンタ１の無線ＬＡＮ通信部のＭＡＣ　ＩＤ，プリンタに装着可能な外部デバイスのＩＤ、上記ＩＤに所定の変換処理を施したもの等を用いる。

【００４２】

（４）プリンタ１０１からのユーザ名を受信する（Ｓ２０９）と、認証サーバ４において、このユーザ名に対応するパスワードが生成され、これを所定のアクセスポイント３を介して送信する（Ｓ２１０）。ＩＥＥＥ８０２．１１ｂにおけるＥＳＳＩＤも送信する（Ｓ２１０）。

（５）プリンタ１０１は上記データを受信すると（Ｓ２１１）、これらを自身の記憶手段に保持し、これらを受信した旨を出力する（Ｓ２１２）。出力は、プリンタ１０１のＬＥＤ等の出力手段に出力してもよいし、受信した旨の情報を送信してアクセスポイント３または認証サーバ４の出力手段に出力するものであってもよい。

【００４３】

（７）所定の時間がたっても上記の出力がない場合（Ｓ２１３）は、再度プリンタ１０１に対応するパスワードを生成し、これを送信する（Ｓ２１０）。これは前回送信したものと同じであってもよいし、異なるものであってもよい。ＥＳＳＩＤも再度送信する（Ｓ２１０）。

（８）上記の出力を確認の後、プリンタ１０１の通信モードをインフラストラクチャモードに設定し、アクセスポイント３の通信モードをインフラストラクチャモードに設定する。これらの設定は、システム管理者の操作によるものでもよいし、プログラムによって自動で行われてもよい（Ｓ２１４）。

【００４４】

（９）プリンタ１０１は上記ユーザ名とパスワードを用いてネットワークに接続する（Ｓ２１５）。

【００４５】

アドホックモードでの通信データは、暗号化データでも平文データでも構わない。

【００４６】

プリンタ１０１を正式にネットワークから切断するときは、システム管理者が認証サーバを操作して、プリンタ１０１を示すユーザをログアウトさせる。

【００４７】

システムに２台以上の上記のプリンタがある場合でも、各プリンタに対して上記の手続きにより、ネットワークに接続できる。各プリンタのＩＤは認証サーバが一元管理しているので、ネットワーク内のどのアクセスポイントを経由しても上記の手続きが可能となる。

【００４８】

パスワードの発行には認証サーバ４にアクセスできる必要がある為，システム管理者だけがパスワードの発行を許可，あるいは発行できる。これらのデータが送受されるアドホックモードの期間は短く、さらにアドホックモードの開始時点はシステム管理者にゆだねられているので、第三者がユーザ名とパスワードを傍受することは困難である。通信チャネルを第三者が知ることも困難である。これにより安全な無線ＬＡＮシステムが維持できる。

【００４９】

また、図１の構成で図４の工程、図３の構成で図２の工程という組み合わせのシステムでも、同様に安全な無線ＬＡＮシステムが維持できる。

【００５０】

（他の実施形態）

以上、本発明の実施形態について詳述したが、本発明は、複数の機器から構成されるシステムに適用しても良いし、また、一つの機器からなる装置に適用しても良い。

【００５１】

なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムを、シス

テム或いは装置に直接或いは遠隔から供給し、そのシステム或いは装置のコンピュータが該供給されたプログラムコードを読み出して実行することによっても達成される場合を含む。その場合、プログラムの機能を有していれば、形態は、プログラムである必要はない。

【００５２】

従って、本発明の機能処理をコンピュータで実現するために、該コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明のクレームでは、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。

【００５３】

その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等、プログラムの形態を問わない。

【００５４】

プログラムを供給するための記録媒体としては、例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）などがある。

【００５５】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続し、該ホームページから本発明のコンピュータプログラムそのもの、もしくは圧縮され自動インストール機能を含むファイルをハードディスク等の記録媒体にダウンロードすることによっても供給できる。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明のクレームに含まれるものである。

【００５６】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布し、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせ、その鍵情報を使用することにより暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

【００５７】

また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される他、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどが、実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現され得る。

【００５８】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現される。

【００５９】

【発明の効果】

以上説明したように本発明によれば、部品コスト・ソフトウェア開発工数の大幅な増加を伴わずに、安全な無線ＬＡＮシステムが、情報入出力装置も含めて構築できる、という効果がある。

【図面の簡単な説明】

【図１】第一実施の形態の無線ＬＡＮシステム構成図である。

【図２】第一実施の形態におけるユーザ名・パスワード割り当ての工程を示すフローチャ

ートである。

【図３】第二実施の形態の無線ＬＡＮシステム構成図である。

【図４】第二実施の形態におけるユーザ名・パスワード割り当ての工程を示すフローチャートである。

【符号の説明】

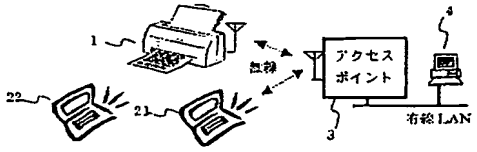
１　無線ＬＡＮ通信機能付きプリンタ

１０１　プリンタ

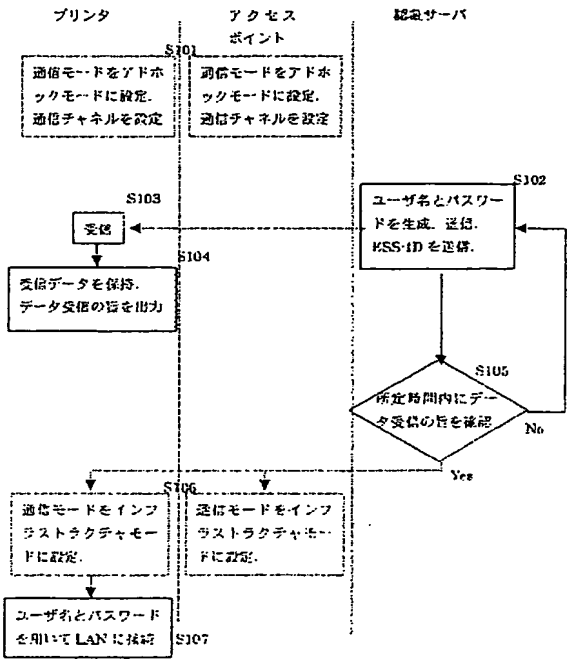
１０２　無線ＬＡＮユニット

２１～２２　コンピュータ

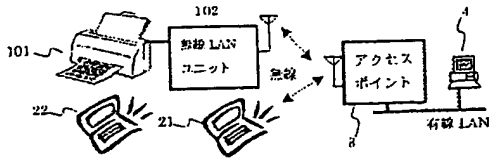
【図１】



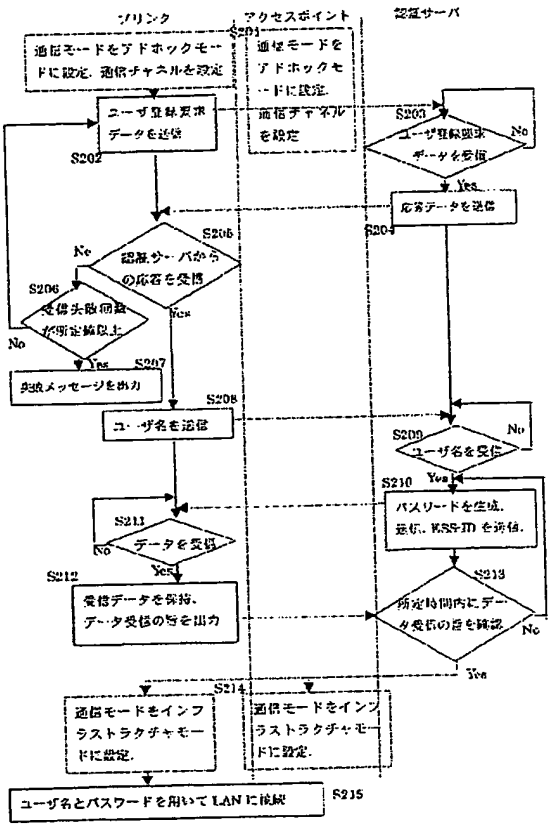
【図２】



【図３】


102
101
無線 LAN
ユニット
無線
アクセス
ポイント
4
有線 LAN
22
21
8

【図４】


プリンタ
アクセスポイント
認証サーバ
通信モードをアドホックモードに設定、通信チャネルを設定
S201
通信モードをアドホックモードに設定、通信チャネルを設定
ユーザ登録要求データを送信
S202
S203
ユーザ登録要求データを受信
No
Yes
応答データを送信
S204
S205
認証サーバからの応答を受信
No
Yes
S206
受信失敗回数が所定値以上
No
Yes
S207
異常メッセージを出力
S208
ユーザ名を送信
S209
ユーザ名を受信
No
Yes
S210
パスワードを生成、暗号、ESS-ID を送信、
S211
データを受信
No
Yes
S212
受信データを保持、データ受信の旨を出力
S213
所定時間内にデータ受信の旨を確認
No
Yes
S214
通信モードをインフラストラクチャモードに設定、
通信モードをインフラストラクチャモードに設定、
ユーザ名とパスワードを用いてLANに接続
S215